Amendments to the Claims

1. (Currently Amended) A method comprising:

after a secure tunnel has been created between a first endpoint and a second endpoint on a packet network which tunnel traverses at least one network address translator (NAT) that, in outgoing packets, sent from the first endpoint to the second endpoint, notes a packet's security association identifier located within the packet and translates a private address of the first endpoint to a shared global address that is not uniquely associated with the first endpoint and, in incoming packets, send from the second endpoint to the shared global address, notes a packet's security association identifier and translates the global address to which the packet is addressed to a private address, which address is determined by heuristically matching the second endpoint's address and incoming security association identifier with the first endpoint's private address and outgoing security association identifier, where mismatches may occur ~~implements a heuristic methodology in translating addresses and/or port numbers, where the heuristic methodology is a methodology in which the NAT translates a private address of the first endpoint to a global address and then attempts to forward to the first endpoint packets sent by the second endpoint to the global address which global address is not uniquely associated with the first endpoint, and where such attempts may fail~~ due to collisions and/or race conditions in the use of security association identifiers, and which tunnel is operating under a secure protocol that is independent of whatever applications are running on the first and second endpoints, and before one or more packets containing application data are sent between the first and second endpoints, sending a control packet from the first endpoint of the tunnel through the tunnel to the second endpoint of the tunnel; and

waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets containing application data through the tunnel

wherein race conditions and collisions in the use of the security association identifiers in forwarding packets sent by the second endpoint to the first endpoint are eliminated or automatic recovery from them is provided.

2. (Cancelled)

3. (Previously Presented) The method of claim 1 wherein the tunnel uses the IPSec security protocol suite.

4. (Original) The method of claim 3 wherein the tunnel uses ESP in tunnel mode.

5. (Cancelled).

6. (Previously Presented) The method of claim 1 wherein the first endpoint is a client and the second endpoint is a server.

7. (Previously Presented) The method of claim 1 wherein the NAT implements VPN Masquerade.

8. (Original) The method of claim 1 wherein the control packet is an ICMP echo request packet and the responsive control packet is an ICMP echo reply packet.

9. (Original) The method of claim 3 wherein the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

10. (Original) The method of claim 9 wherein before the end of tunnel's lifetime the endpoints establish a new tunnel between them.

11. (Previously Presented) The method of claim 10 wherein a designated one of the endpoints has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish a new tunnel.

12. (Original) The method of claim 1 wherein the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets.

13. (Previously Presented) The method of claim 1 wherein if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends another control packet through the tunnel to the second endpoint.

14. (Original) The method of claim 13 wherein if the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint.

15. (Previously Presented) The method of claim 10 wherein if one of the endpoints is unable to complete the establishment of a new tunnel to the other endpoint before a predetermined time limit then that one endpoint abandons establishment of that tunnel and starts establishing a new tunnel to the other endpoint.

16. (Previously Presented) The method of claim 15 wherein if the one of the endpoints successively fails to establish a new tunnel for more than a predetermined maximum number of times to the other endpoint then that one

endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection.

17. (Original) The method of claim 16 wherein the connection used to establish tunnels between the endpoints is an IKE session.

18. (Currently Amended) A computer readable media tangibly embodying a program of instructions executable by a computer to perform a method, the method comprising:

after a secure tunnel has been created between a first endpoint and a second endpoint on a packet network which tunnel traverses at least one network address translator (NAT) that, in outgoing packets, sent from the first endpoint to the second endpoint, notes a packet's security association identifier located within the packet and translates a private address of the first endpoint to a shared global address that is not uniquely associated with the first endpoint and, in incoming packets, send from the second endpoint to the shared global address, notes a packet's security association identifier and translates the global address to which the packet is addressed to a private address, which address is determined by heuristically matching the second endpoint's address and incoming security association identifier with the first endpoint's private address and outgoing security association identifier, where mismatches may occur ~~implements a heuristic methodology in translating addresses and/or port numbers, where the heuristic methodology is a methodology in which the NAT translates a private address of the first endpoint to a global address and then attempts to forward to the first endpoint packets sent by the second endpoint to the global address which global address is not uniquely associated with the first endpoint, and where such attempts may fail~~ due to collisions and/or race conditions in the use of security association identifiers, and which tunnel is operating under a secure protocol that is independent of whatever applications are running on the first and second endpoints, and before one or more packets containing application data are sent between the first and second endpoints,

sending a control packet from the first endpoint of the tunnel through the tunnel to the second endpoint of the tunnel; and

waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets containing application data through the tunnel

wherein race conditions and collisions in the use of the security association identifiers in forwarding packets sent by the second endpoint to the first endpoint are eliminated or automatic recovery from them is provided.

19. (Cancelled)

20. (Previously Presented) The computer readable media of claim 18 where in the method the tunnel uses the IPSec security protocol suite.

21. (Original) The computer readable media of claim 20 where in the method the tunnel uses ESP in tunnel mode.

22. (Cancelled)

23. (Previously Presented) The computer readable media of claim 18 where in the method the first endpoint is a client and the second endpoint is a server.

24. (Previously Presented) The computer readable media of claim 18 where in the method the NAT implements VPN Masquerade.

25. (Original) The computer readable media of claim 18 where in the method the control packet is an ICMP echo request packet and the responsive control packet is an ICMP echo reply packet.

26. (Original) The computer readable media of claim 20 where in the method the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

27. (Original) The computer readable media of claim 26 where in the method before the end of tunnel's lifetime the endpoints establish a new tunnel between them.

28. (Previously Presented) The computer readable media of claim 27 where in the method a designated one of the endpoints has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish a new tunnel.

29. (Original) The computer readable media of claim 18 where in the method the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets.

30. (Previously Presented) The computer readable media of claim 18 where in the method if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends another control packet through the tunnel to the second endpoint.

31. (Original) The computer readable media of claim 30 where in the method if the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint.

32. (Previously Presented) The computer readable media of claim 27 where in the method if one of the endpoints is unable to complete the establishment of a new tunnel to the other endpoint before a predetermined time limit then that one endpoint abandons establishment of that tunnel and starts establishing a new tunnel to the other endpoint.

33. (Previously Presented) The computer readable media of claim 32 where in the method if the one of the endpoints successively fails to establish a new tunnel for more than a predetermined maximum number of times to the other endpoint then that one endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection.

34. (Original) The computer readable media of claim 33 where in the method the connection used to establish tunnels between the endpoints is an IKE session.